Result Page

Description procedure and device for implementing a byte substitution operation of the AES algorithm after Rijndael the available invention refers to the AES algorithm after Rijndael and in particular to an improved implementation of the byte substitution operation of this algorithm.

Fig. a general chart for the AES cryptoalgorithm, which is called also Rijndael algorithm, shows 6. The Rijndael algorithm is in the document " The Rjindael block Cipher: AES Proposal " of Joan Daemen and Vincent Rijmen, document version 2,9. March 1999, described.

The AES algorithm is an iterative algorithm, with which a given amount of (10.12 or 14) is computed by rounds (rounds). Becomes following on the basis Fig. 6 a round < RTI ID=1.1> AES Algorithmus< /RTI> for a mode exemplary represented.

Starting point of a round is a block of 16 bytes, whereby each byte < RTI ID=1.2> 8< /RTI> Bit a block of < enclosure, thus; RTI ID=1.3> 8< /RTI> x 16 bits. These are in Fig. 6 with 600 as vertical lines represented. The AES algorithm or Rijndael algorithm is a so-called block Cipher algorithm, with with in Fig. 6 example shown a block of 16 x 8 bits at input data to be coded together.

The first step of a round is < RTI ID=1.4> as " Add< /RTI> Round key " (add the key for a round) designates. This function is symbolized by the circles represented with 620. The AES Rundenschlüssel, which is usually derived from a AES key and as Expanded key is designated, covers likewise 16 x 8-bits. In the stage ADD Round key is accomplished a XOR coding bit by bit with the AES round key and the 16 x 8-bits at input data, as it is represented with 630.

The next < RTI ID=2.1> Verarbeitungsstufe< /RTI> a round < RTI ID=2.2> AES < /RTI> Algorithm exists those in a byte substitution, in Fig. 6 as byte Sub one designates. The byte substitution exists in a mathematical function, which covers a multiplicative inverse one with affiner illustration with the AES algorithm.

This mathematical function is implemented by a turn consulting, which is usually called S-box and in Fig. 6 by cubes 640 is symbolically represented. The original data of the stage 620 become as address for the S-box, D. h. the byte substitution turn consulting, uses, in order to spend as original data on each byte a substitution byte, which is the multiplicative inverse one with affiner illustration of the entrance address. The S-box contains no secret information, but can in advance be computed or by a publicly accessible place be called up. The secret information is D in the input data. h. Entrance addresses for < RTI ID=2.3> S-Box.< /RTI>

The original data of the byte substitution < RTI ID=2.4> 640< /RTI> , those are then submitted of a line shift operation 650 in Fig. 6 as " SHIFTs Row " one designates. The original data of the stage 650 are then submitted of a column mixture, those in Fig. 6 by oblong right parallelepipeds is symbolically represented and in the technology as " mixes Column " is designated. The operations 620.640, 650 and 660 form one of typically ten rounds < RTI ID=2.5> AES algorithm, < /RTI> whereby a round in the technology also as Round is designated. The original data of the mix Column operation, D. h. , again an ADD Round key operation 620 ' is then submitted of a round or a Round, whereby again a XOR linkage bit by bit of the data with a key < RTI ID=2.6> 630 ' für< /RTI> the next round is accomplished etc. After a selectable number of rounds, which usually 10 amounts to, lie then < RTI ID=2.7> AES verschlüsselten< /RTI> Data forwards.

Unfavorably to above described execution byte substitution by means of turn consulting is that in a coding mechanism, in which input data are transformed into substituted data thus in the mechanism 640 of Fig. 6, another table to be used must, than in a decoding mechanism, in which the corresponding inverse operation of the symmetrical AES algorithm, thus a back substitution of the data, is accomplished. A device, which accomplishes both a coding and a decoding in accordance with the AES algorithm after Rijndael, needs thus two turn consulting, i.e. one for the coding component and one for the decoding component. It is pointed out that the byte substitution turn consulting is large 256 x 8 bits, thus 256 byte. A well-known device needs therefore 2 x 256 byte storage location for storing the byte substitution table.

▲ top

The above memory data apply to a serial Berchnung of the byte substitution. From speed reasons however usually a parallel processing becomes the z. B. 16 bytes assigned. Then must < RTI ID=3.1> Bytesubstitutionstabelle< /RTI> 16-fach available its. The necessary storage location amounts to then 16 x 2 x 256 byte.

For applications of the AES algorithm on general-purpose computers this no substantial problem represents. Completely differently the situation behaves however with smart cards, with which due to the size of the memory chip very restrictive storage requests are present. The memory on smart cards lies within the range of kilobyte, so that the byte substitution tables for the decoding component and for the coding component of the circuit take a substantial storage location up. On the other hand the algorithms which can be required on a smart card are more and more complex, so that also the requirements rise regarding the main memory of the smart card, so that the smart card can compute also more complex algorithms with a reasonable throughput. The task of the available invention consists of it, < RTI ID=4.1> ef-< /RTI> to create fizienteres concept for implementing a byte substitution operation of the AES algorithm after Rijndael.

This task is < by a procedure in accordance with patent claim; RTI ID=4.2> 1, < /RTI> by a device in accordance with patent claim 7 or by a cryptography system in accordance with patent claim 8 solved.

The available invention is the basis the realization that the byte substitution operation z. B. < RTI ID=4.3> AES Algorithmus< /RTI> after Rijndael to be split up must and partly by a hard-wired arithmetic unit and partly z. B. by a turn consulting or otherwise to accomplish is. The byte substitution operation consists of two partial operations, i.e. the operation of the multiplicative inverse ones and the partial operation of the affinen illustration. In analogy to it the byte substitution operation in a decoding device in a partial operation of the inverse affinen illustration and in the partial operation of the multiplicative inverse ones exists.

The affine illustration is implemented according to invention by means of a hard-wired arithmetic unit, while the multiplicative inverse one z. B. by means of a turn consulting one determines. This makes it that both for the coding operation and for the decoding operation the same turn consulting can be used, i.e. simply the turn consulting for the multiplicative inverse one possible.

A cryptography device with one < RTI ID=4.4> Entschlüsselungskom < /RTI> ponente and a coding component must store therefore only still another only one turn consulting for the byte substitution operation, which results in a memory saving of for example 16 x 256 byte for a parallel implementation. For larger turn consulting, D. h., if the AES algorithm does not < RTI ID=4.5> byte by byte, sondern< /RTI> on larger data blocks, is still more significant memory saving is implemented in byte.

If the computation of the multiplicative inverse ones is accomplished in other way than by a turn consulting, then the available invention is favourable in the fact that z. B. only one arithmetic unit or only one software program both for the coding and the decoding to be needed.

In the turn consulting thus not the usually available S-box-values, but only a table of the multiplicative inverse ones of the initially (address) are put down according to invention values. In a further step the affine illustration is then realized hard-wired. A preferential wiring consists of using only XOR gates whereby in a further arrangement of the available invention XOR gates with two entrances are only used, in order to limit the number of necessary transistors.

Thus the same table can to be used for coding and decoding and it not have two separate tables with 256 < RTI ID=5.1> x< /RTI> 8 bits gespeichert'werden.

Preferential remark examples of the available invention are more near described in the following referring to the enclosed designs. Show: Fig. < RTI ID=5.2> 1< /RTI> a block diagram of a according to invention before direction for implementing a Bytesubstitutionsope ration of the AES algorithm after Rijndael for those
Coding operation; Fig. 2 a block diagram of a device for implementing a byte substitution operation of the AES
Algorithm after Rijndael for the decoding operation; Fig. 3a the calculation specification for the affine illustration; Fig. 3b a arithmetic-logical representation of the before writing of Fig. 3a; Fig. 4 an arithmetic unit for the calculation of the affinen illustration in accordance with a first remark example of the vorlie genden invention; Fig. 5 an arithmetic unit for the calculation of the affinen illustration in accordance with a further remark example before lying invention; and Fig. 6 a general chart over a round of the AES
Algorithm.

The byte substitution operation of the AES algorithm is a nonlinear byte substitution, which affects each of the status bytes of the AES algorithm independently. The substitution table (or S-box) consists of two transformations.

First the multiplicative inverse one in AP must < RTI ID=6.1> (28) < /RTI> are determined, and then the result data of a affinen must < RTI ID=6.2> Transformation (over AP (2)) submitted werden.< /RTI>

The device covers a mechanism 10 according to invention for implementing the byte substitution operation first for implementing the partial operation of the multiplicative inverse ones by means of a turn consulting and then a hard-wired arithmetic unit 12 for the calculation of the affinen illustration of the original data of the mechanism 10, in order to receive from input data at an entrance 14 substituted data at an exit 16.

During Fig. < RTI ID=6.3> 1< /RTI> to a coding device, is Fig applies. 2 for a decoding device represented. Substituted data are supplied first to an arithmetic unit 20, which is hard-wired. The arithmetic unit computes the inverse affine illustration. The original data of the mechanism 20 are then supplied to a mechanism 22 for the calculation of the multiplicative inverse ones. The mechanism < RTI ID=7.1> 22< /RTI> is again, like the mechanism 10 of Fig. 1, when turn consulting for the multiplicative inverse one organizes. At an exit 24 in Fig. 2 device shown is present thus backsubstituted data, those from substituted data at an entrance 26 in Fig. 2 device shown computed is.

In the following becomes referring to Fig. 3a on the Be< RTI ID=7.2> rechnungsvorschrift< /RTI> to the calculation of the affinen illustration received. Fig. 3a represents thus the calculation specification, those the arithmetic unit 12 from Fig. < RTI ID=7.3> 1< /RTI> to convert must. The input data into the arithmetic unit are named xo to X7, while the original data from the arithmetic unit, thus the substituted data of Fig. 1, with < RTI ID=7.4> yo< /RTI> until y7 are designated. It is pointed out that the affine illustration in Fig. 3a for eight entrance bits and eight output bits is represented. It is however also pointed out that the AES algorithm could be implemented also in principle with another number of bits per block.

By inversion of the vector equation, those in Fig. 3a is shown, becomes the mathematical regulation the calculation of the inverse affinen illustration, those by the arithmetic unit 20 of Fig. 2 to implement is received.

Fig. 3b shows the computation regulation such measuring of Fig. 3a by means of logical operators, whereby the indication stands + for a XOR linkage, while indication for one Not or emergency operation stands. The addition, those by the last column of Fig. 3a represented is, can in the binary system also by the emergency operation be computed, depending on, what is technical circuiting more favorable.

Fig. a technical circuiting realization shows 4 in Fig. 3b equations shown. As input values xo are < RTI ID=8.1> to x7< /RTI> entered, over as initial values < RTI ID=8.2> yo< /RTI> to < RTI ID=8.3> y< /RTI> to receive.

In Fig. eight XOR gates 40 to 47 cover 4 circuit shown, whereby the exits of the XOR gates 40.41, 45 and 46, like it by in Fig. 3b appropriate equations shown is given, is inverted.

Like it from Fig. 4 to see is, has everyone of the XOR gates 40 to 47 more than two entrances.

A more transistor-saving implementation in Fig. 3b computation regulation shown is in Fig: 5 represented. Fig.

covers 5 again excluding XOR gates 50 to 65, whereby however all gates have an exit excluding two entrances and. By means of the XOR gates 50 to 53 first auxiliary variables Hl to H4 are computed. By means of the XOR gates 54 to 57 from the first auxiliary variables H1 to H4 second auxiliary variables H5 to H8 are then computed. The initial values, thus the substituted data at the exit 16 of Fig. < RTI ID=8.4> 1< /RTI> and/or. yo to < RTI ID=8.5> y7, < /RTI> by the XOR gates 58 to 65 it is finally received, whereby the exits of the XOR gates 58.59, 63 and 64 are inverted, like it by in Fig. 3b equations shown is given.

Although in Fig. 5 circuit shown more XOR gates than in Fig. , is preferred nevertheless it exhibits 4 circuit shown, there everyone in Fig. 5 XOR gates shown of only two entrances exhibits, so that altogether a transistor saving can be achieved.

It is pointed out that further technical circuiting implementations of the partial operation of the affinen illustration and/or. the inverse affinen illustration to be implemented can.

Independently of it, which is selected special implementation for the hard-wired arithmetic unit for the calculation of the affinen illustration, or whether the computation of the affinen Abbil dung is implemented by software, always the advantage is received that both the decoding component and the coding component of a cryptography device can use the same turn consulting, in which the multiplicative inverse one is tabular stored.

Reference symbol list 10 mechanism for implementing the partial operation mul inverse ones 12 arithmetic unit tiplikativen for the calculation of the affinen illustration 14 entrance of a coding mechanism 16 exit of the coding mechanism 20 arithmetic unit for the calculation of the inverse affinen illustration 22 mechanism for implementing the partial operation mul tiplikativen inverse ones by means of a turn consulting 24 exit of the decoding mechanism 26 entrance of the decoding mechanism < RTI ID=10.1> 40-47< /RTI> XOR gate with more than two entrances < RTI ID=10.2> 50-57< /RTI> first sentence of XOR gates with two entrances < RTI ID=10.3> 58-65< /RTI> second sentence of XOR gates with two entrances 600 entrance byte 620 ADD Round key function 630 XOR coding with the AES Rundenschlüssel 640 byte substitution operation by means of a S-box 650 SHIFT Row function 660 mix Column function 620 ' ADD Round key function of the next round < RTI ID=10.4> 630 ' XOR Verschlüsselung< /RTI> for the next round

Result Page

Patent claims < RTI ID=11.1> 1.< /RTI> Procedure for implementing a byte substitution operation, whereby the byte substitution operation exhibits a partial operation of the affinen illustration and a partial operation of the multiplicative inverse ones, with the following steps: Implement < RTI ID=11.2> (10) < /RTI> the partial operation of the multiplicative inverse ones; and implementing (12) the partial operation of the affinen illustration by means of an arithmetic unit.

2. Procedure according to requirement < RTI ID=11.3> 1, < /RTI> with that < RTI ID=11.4> Bytesubstitutions < /RTI> operation the byte substitution operation < RTI ID=11.5> AES Algorithmus< /RTI> after Rijndael is.

3. Procedure according to requirement 1 or 2, with which der'Schritt implementing (10) the partial operation of the multiplicative inverse ones by means of a turn consulting one accomplishes.

4. Procedure in accordance with one of the preceding requirements, with which the arithmetic unit is for the calculation of the partial operation of the affinen illustration a CCU and which is implemented computation in software.

5. Procedure in accordance with one of the requirements 1 to 3, with which the arithmetic unit is for the calculation of the affinen illustration a hard-wired arithmetic unit.

6. Procedure in accordance with requirement 5, with which the hard-wired arithmetic unit exhibits XOR gates for implementing the partial operation of the affinen illustration only.

7. Procedure in accordance with requirement 6, with which each XOR gate of the hard-wired arithmetic unit exhibits only two entrances and an exit.

8. Procedure in accordance with requirement 7, with which a data input block for < RTI ID=12.1> Bytesubstitutionsope < /RTI> ration a number of bits exhibits and a data output block for the byte substitution operation the same number of bits exhibits, and with which the step of implementing the partial operation of the affinen illustration exhibits the following steps: Compute a number of auxiliary variables < RTI ID=12.2> (Hl-H8) < /RTI> using a first sentence of XOR gates (50-57) with exactly in each case two entrances, whose number is equal to the number of auxiliary variables, whereby the number of auxiliary variables is equal to the number of bits of the data input block; and calculation of the bits < RTI ID=12.3> (yo-y) < /RTI> the data output block using a second sentence of XOR gates < RTI ID=12.4> (58-65) < /RTI> with in each case two entrances using the Bits'des of data input block and the auxiliary variables, whereby the number of XOR is gate (58-65) of the second sentence equal to the number of bits of the data output block.

▲ top < RTI ID=12.5> 9.< /RTI> Device for implementing a byte substitution operation, whereby the byte substitution operation exhibits a partial operation of the affinen illustration and a partial operation of the multiplicative inverse ones, with the following characteristics: a mechanism for implementing (10) the partial operation of the multiplicative inverse ones; and a mechanism for implementing (12) the partial operation of the affinen illustration by means of an arithmetic unit.

10. Symmetrical cryptography system for implementing a coding operation and a decoding operation using an algorithm, which exhibits a byte substitution operation, which exhibits a partial operation of the affinen illustration and a partial operation of the multiplicative inverse ones, with the following characteristics: in a coding mechanism: a mechanism for implementing the partial operation mul inverse ones tiplikativen; and an arithmetic unit < RTI ID=13.1> (12) < /RTI> to implementing the partial operation of the affinen illustration; in a decoding mechanism: an arithmetic unit (20) to implementing an operation, to
Partial operation of the affinen illustration is inverse; and a mechanism (22) for implementing the partial operation of the multiplicative inverse ones, whereby the mechanism (10) as implementing the partial operation of the multiplicative inverse ones is trained in the coding mechanism and the decoding mechanism, in order to use only one mechanism together, by which the partial operation of the multiplicative inverse ones is assignable.

11. Symmetrical cryptography system according to requirement 10, with which the only mechanism exhibits only one turn consulting, in which the partial operation of the multiplicative inverse ones is tabular stored